

Artificial-Noise-Aided Transmission in Multi-Antenna Relay Wiretap Channels with Spatially Random Eavesdroppers

Chenxi Liu, *Student Member, IEEE*, Nan Yang, *Member, IEEE*,
Robert Malaney, *Member, IEEE*, and Jinhong Yuan, *Senior Member, IEEE*

Abstract—We design a new secure transmission scheme in the relay wiretap channel where a source communicates with a destination through a decode-and-forward relay in the presence of spatially random-distributed eavesdroppers. For the sake of practicality, we consider a general antenna configuration in which the source, relay, destination, and eavesdroppers are equipped with multiple antennas. In order to confuse the eavesdroppers, we assume that both the source and the relay transmit artificial noise signals in addition to information signals. We first derive a closed-form expression for the transmission outage probability and an easy-to-compute expression for the secrecy outage probability. Notably, these expressions are valid for an arbitrary number of antennas at the source, relay, and destination. We then derive simple yet valuable expressions for the asymptotic transmission outage probability and the asymptotic secrecy outage probability, which reveal the secrecy performance when the number of antennas at the source grows sufficiently large. Using our expressions, we quantify a practical performance metric, namely the secrecy throughput, under a secrecy outage probability constraint. We further determine the system and channel parameters that maximize the secrecy throughput, leading to analytical security solutions suitable for real-world deployment.

Index Terms—Physical layer security, wiretap channel, relay, secrecy outage, stochastic geometry, artificial noise.

I. INTRODUCTION

SECURITY is a vital issue in wireless communication networks since data transmissions over the shared physical medium are inherently vulnerable to potential eavesdropping. Traditionally, security in wireless communication networks is realized by cryptographic techniques applied to the upper layers utilizing secret keys. The secrecy provided by such techniques is achieved under the assumption of finite computational capability at the eavesdroppers. However, this assumption cannot be easily satisfied with the rapid and continuous growth of the computational capability of modern processors, which makes the traditional cryptographic techniques increasingly weak. Moreover, the ever-expanding size of decentralized wireless networks introduces significant challenges

to key distribution and management. Against this backdrop, physical layer security has been proposed as a complementary technique to traditional cryptography, due to its benefits in enhancing the secrecy level of wireless communications by direct exploiting the randomness offered by wireless channels [1, 2]. In seminal studies, e.g., [3], it was established in a single-input single-output wiretap channel that secrecy can only exist when the wiretap channel between the source and the eavesdropper is a degraded version of the main channel between the source and the legitimate receiver. This result was later generalized to the case where the main channel and the wiretap channel are independent [4].

Deploying multiple antennas at the source and/or the legitimate receiver has been shown to effectively boost the physical layer security of wiretap channels [5–17]. The effectiveness of multiple antennas relies on the use of secure multi-input multi-output (MIMO) techniques, such as beamforming [5–9], artificial noise (AN) [10–13], and transmit antenna selection [14–17]. In the MIMO setting, the presence of randomly distributed eavesdroppers has been recently investigated [18–22]. In order to statistically characterize the secrecy performance of such scenarios, stochastic geometry and random geometric graphs are often used to model the locations of spatially random-distributed nodes. With such modeling, [18] investigated the throughput of large-scale decentralized wireless networks with physical layer security constraints. Considering the path loss as the sole factor affecting the received signal-to-noise ratios (SNRs) at the legitimate receiver and the eavesdropper, [19] examined the secrecy rate in cellular networks. In [20] and [21], the secrecy rate achieved by linear precoding was analyzed for the broadcast channel and the cellular network, respectively. In [22], the impact of AN was investigated.

The above works [5–22] examine physical layer security in point-to-point MIMO systems. Cooperative relaying, on the other hand, is another promising and widely-adopted technique that efficiently improves the coverage and reliability of wireless networks [23, 24]. In order to enhance physical layer security in relay wiretap channels, a variety of approaches have been investigated such as cooperative beamforming [25–28], relay selection [29, 30], and cooperative jamming [31, 32]. However, a common limitation of [25–32] is that they only considered fixed locations of eavesdroppers. This leaves open the problem of designing relay-aided secure transmission schemes for the scenario where the locations of eavesdroppers are spatially randomly distributed.

The work of R. Malaney and J. Yuan was supported by the Australian Research Council Discovery Project (DP120102607). The work of N. Yang was supported by the Australian Research Council Discovery Project (DP150103905).

C. Liu, R. Malaney, and J. Yuan are with the School of Electrical Engineering and Telecommunications, The University of New South Wales, Sydney, NSW 2052, Australia (email: chenxi.liu@student.unsw.edu.au; r.malaney@unsw.edu.au; j.yuan@unsw.edu.au).

N. Yang is with the Research School of Engineering, Australian National University, Canberra, ACT 0200, Australia (email: nan.yang@anu.edu.au).

In this work we design a new relay-aided secure transmission for the relay wiretap channel. In such a channel, the communication between the source and the destination is aided by a decode-and-forward (DF) relay and overheard by multiple spatially random-distributed eavesdroppers. We focus on the general scenario where the source, the relay, the destination, and the eavesdroppers are equipped with multiple antennas, which stands as a major advancement over the previous studies on securing the relay wiretap channel [25–32]. In order to confuse the eavesdroppers, we assume that in the secure transmission the source and the relay transmit AN signals together with information signals in the first hop and the second hop, respectively¹. The contributions made by this work are summarized as follows:

- 1) We derive a closed-form expression for the transmission outage probability and an easy-to-compute expression for the secrecy outage probability. Notably, both expressions are independent of realizations of channels and valid for an arbitrary number of antennas at the source, relay, and destination. Moreover, these expressions serve as the key results that enable us to explicitly characterize the secrecy throughput of the considered relay wiretap channels.
- 2) We derive simple yet valuable expressions for the asymptotic transmission outage probability and the asymptotic secrecy outage probability. These expressions quantify the secrecy performance in the regime where the number of antennas at the source becomes sufficiently large. Based on our analysis, we find that the asymptotic transmission outage probability is determined by the average SNR of the relay-destination channel only. We also find that the asymptotic secrecy outage probability approaches a certain value which is independent of the number of antennas at the source.
- 3) We determine the transmission parameters, i.e., the wiretap code rates and the power allocation factors, that maximize the secrecy throughput of the considered relay wiretap channels under a secrecy outage probability constraint. Moreover, we demonstrate the effectiveness of the determined transmission parameters on maximizing the secrecy throughput. Furthermore, we evaluate the impact of the system parameters, e.g., the number of antennas and the density of eavesdroppers, on the secrecy throughput.

Beyond the above contributions, we provide some pivotal insights into the practical design of secure transmission. First, we show that the AN signals from the source play a more dominant role in securing the transmission in the considered relay wiretap channels than the AN signals from the relay. Second, we show that adding extra antennas at the source significantly increases the maximum secrecy throughput, but does not decrease the secrecy outage probability always. Third, we find that in order to achieve the maximum secrecy throughput, the

¹An initial study of a much simpler system model is given in [33] where the relay, the destination, and the eavesdroppers are all equipped with a single antenna and AN signals are transmitted by the source in the first hop only. This simplified system configuration allowed for analytical tractability at the expense of significant sub-optimality.

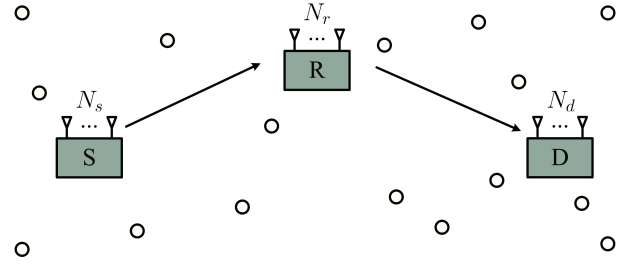


Fig. 1. Illustration of a relay wiretap channel in the presence of spatially random multi-antenna eavesdroppers.

source needs to allocate a higher power to AN signals whereas the relay needs to allocate a lower power to AN signals when the antenna number at the source increases. Fourth, we find that the maximum secrecy throughput increases when the eavesdroppers are more dispersed.

The rest of the paper is organized as follows. Section II describes the relay wiretap channel considered in the paper. In Section III, we derive expressions for the outage probabilities of the considered relay wiretap channel. The characterization and maximization of the secrecy throughput are also provided in Section III. Numerical results and related discussions are presented in Section IV. Finally, Section V draws conclusions.

Notations: Column vectors (matrices) are denoted by bold-face lower (upper) case letters. Conjugate transpose is denoted by $(\cdot)^H$. The determinant of a matrix is denoted by $\det(\cdot)$. Complex Gaussian distribution is denoted by \mathcal{CN} . A zero matrix and an identity matrix of appropriate dimension are denoted by $\mathbf{0}$ and \mathbf{I} , respectively. Statistical expectation is denoted by \mathbb{E} . The Frobenius norm of a vector or a matrix is denoted by $\|\cdot\|$.

II. MULTI-ANTENNA RELAY WIRETAP CHANNEL

We consider a relay wiretap channel, as depicted in Fig. 1, where a source (S) communicates with a destination (D) with the aid of a relay (R) in the presence of multiple spatially random eavesdroppers. In this channel, the source, the relay, the destination, and each eavesdropper are equipped with N_s , N_r , N_d , and N_e antennas, respectively. We denote \mathbf{H}_{sr} as the $N_r \times N_s$ channel matrix from the source to the relay and denote \mathbf{H}_{rd} as the $N_d \times N_r$ channel matrix from the relay to the destination. We consider that all the channels are subject to independent and identically distributed (i.i.d) Rayleigh fading. We also consider a quasi-static block fading environment in which all the channel coefficients remain the same within one time slot. We assume that the channel state information (CSI) between the source and the relay and the CSI between the relay and the destination are known at the source, while the CSI from the eavesdroppers is not known. We also assume that $N_s > N_e$, mimicking the case where the source is a base station (BS) with a large number of antennas, while the eavesdroppers are mobile users with a limited number of antennas. We further assume that the destination is located remotely away from the source such that the destination cannot receive signals from the source directly. All the nodes operate in a half-duplex mode such that each node cannot

transmit and receive simultaneously. We denote d_{sr} and d_{rd} as the source-relay distance and the relay-destination distance, respectively, and denote η as the path loss exponent. The locations of the eavesdroppers are modeled as a homogeneous Poisson Point Process (PPP) Φ with density λ [18–22], which represents the case where the eavesdroppers are mobile users in a decentralized network [34]. We clarify that the source, the relay, and the destination do not belong to Φ .

A. Transmission of Artificial Noise Signals

We now detail the transmission scheme between the source and the destination. In this scheme we assume that both the source and the relay transmit AN signals together with the information signals. This scheme utilizes two time slots. In the first time slot, the source transmits information signals and AN signals to the relay, referred to as the first hop transmission. We assume that the relay adopts maximum-ratio combining (MRC) [35–37] to process the received signals in order to maximize the received SNR. In the second time slot, the DF relay transmits the re-encoded signals and AN signals to the destination, referred to as the second hop transmission. We assume that the destination also adopts MRC to process the received signals. In the second time slot, it is assumed that the source transmits AN signals to further confuse the eavesdropper. We clarify that both the first hop transmission and the second hop transmission are overheard by the eavesdroppers.

In the first hop transmission, the signal transmitted by the source is given by

$$\mathbf{x}_S = \mathbf{W}_1 \mathbf{t}_1, \quad (1)$$

where \mathbf{W}_1 denotes the $N_s \times N_s$ beamforming matrix at the source and \mathbf{t}_1 denotes the combination of the information signal and the AN signal at the source. To transmit \mathbf{x}_S , we first design \mathbf{W}_1 as

$$\mathbf{W}_1 = [\mathbf{w}_S \quad \mathbf{W}_{\text{SAN}}], \quad (2)$$

where \mathbf{w}_S is used to transmit the information signal at the source and \mathbf{W}_{SAN} is used to transmit the AN signal at the source. The aim of \mathbf{W}_1 is to degrade the quality of the received signals at the eavesdroppers. By transmitting AN signals through \mathbf{W}_1 , together with the fact that the relay adopts MRC to process the received signals from the source, we ensure that the quality of the received signals at the relay is free from AN interference. In designing \mathbf{W}_1 , we choose \mathbf{w}_S as the eigenvector corresponding to the largest non-zero eigenvalue of $\mathbf{H}_{sr}^H \mathbf{H}_{sr}$, denoted by $\lambda_{\text{max}}^{sr}$. We then choose \mathbf{W}_{SAN} as the remaining $N_s - 1$ eigenvectors of $\mathbf{H}_{sr}^H \mathbf{H}_{sr}$. Such design ensures that \mathbf{W}_1 is a unitary matrix. We then design \mathbf{t}_1 as

$$\mathbf{t}_1 = \begin{bmatrix} t_S \\ \mathbf{t}_{\text{SAN}} \end{bmatrix}, \quad (3)$$

where t_S denotes the information signal at the source and \mathbf{t}_{SAN} is an $(N_s - 1) \times 1$ vector of the AN signal at the source. We define β_s , $0 < \beta_s \leq 1$, as the fraction of the power allocated to the information signal at the source. As such, we

have $\mathbb{E}[|t_S|^2] = \beta_s$ and $\mathbb{E}[\mathbf{t}_{\text{SAN}} \mathbf{t}_{\text{SAN}}^H] = \frac{1-\beta_s}{N_s-1} \mathbf{I}_{N_s-1}$. Based on (1), (2), and (3), the received signal at the relay in the first hop transmission is expressed as

$$y_r = \sqrt{P_s d_{sr}^{-\eta}} \mathbf{H}_{sr} (\mathbf{w}_S t_S + \mathbf{W}_{\text{SAN}} \mathbf{t}_{\text{SAN}}) + \mathbf{n}_r, \quad (4)$$

where P_s denotes the transmit power at the source and \mathbf{n}_r denotes the thermal noise at the relay, the elements of which are assumed to be i.i.d complex Gaussian random variables with zero mean and variance σ_r^2 , i.e., $\mathbf{n}_r \sim \mathcal{CN}(\mathbf{0}_{N_r}, \sigma_r^2 \mathbf{I}_{N_r})$. We note that AN signals in (4) can be canceled at the relay by applying MRC.

We next express the received signal at a typical eavesdropper located at i , $i \in \Phi$, in the first hop transmission as

$$\mathbf{y}_i^{(1)} = \sqrt{P_s d_{si}^{-\eta}} \mathbf{H}_{si} (\mathbf{w}_S t_S + \mathbf{W}_{\text{SAN}} \mathbf{t}_{\text{SAN}}) + \mathbf{n}_{i1}, \quad (5)$$

where \mathbf{H}_{si} denotes the $N_e \times N_s$ channel matrix from the source to the typical eavesdropper located at i , d_{si} denotes the distance between the source and the typical eavesdropper located at i , and \mathbf{n}_{i1} denotes the thermal noise vector at the typical eavesdropper located at i , the elements of which are assumed to be i.i.d complex Gaussian random variables with zero mean and variance σ_{i1}^2 , i.e., $\mathbf{n}_{i1} \sim \mathcal{CN}(\mathbf{0}_{N_e}, \sigma_{i1}^2 \mathbf{I}_{N_e})$.

In the second time slot, the DF relay first decodes the received signals from the source. If the received signals are successfully decoded, the relay retransmits the re-encoded signals and AN signals to the destination. The signals transmitted by the relay is given by

$$\mathbf{x}_R = \mathbf{W}_2 \mathbf{t}_2, \quad (6)$$

where \mathbf{W}_2 denotes the $N_r \times N_r$ beamforming matrix at the relay and \mathbf{t}_2 denotes the combination of the information signal and the AN signal at the relay. Similar to \mathbf{W}_1 and \mathbf{t}_1 , we design \mathbf{W}_2 and \mathbf{t}_2 as

$$\mathbf{W}_2 = [\mathbf{w}_R \quad \mathbf{W}_{\text{RAN}}], \quad (7)$$

and

$$\mathbf{t}_2 = \begin{bmatrix} t_R \\ \mathbf{t}_{\text{RAN}} \end{bmatrix}, \quad (8)$$

respectively. In (7), \mathbf{w}_R is used to transmit the information signal at the relay and \mathbf{W}_{RAN} is used to transmit the AN signal at the relay. In designing \mathbf{W}_2 , we choose \mathbf{w}_R as the eigenvector corresponding to the largest eigenvalue of $\mathbf{H}_{rd}^H \mathbf{H}_{rd}$, denoted by $\lambda_{\text{max}}^{rd}$. We then choose \mathbf{W}_{RAN} as the remaining $N_r - 1$ eigenvectors of $\mathbf{H}_{rd}^H \mathbf{H}_{rd}$. This design ensures that the quality of the received signals at the destination is free from AN interference when the destination applies MRC to process the received signals. In (8), t_R denotes the information signal at the relay and \mathbf{t}_{RAN} is an $(N_r - 1) \times 1$ vector of the AN signals at the relay. We define β_r , $0 < \beta_r \leq 1$, as the fraction of the power allocated to the information signals at the relay. As such, we have $\mathbb{E}[|t_R|^2] = \beta_r$ and $\mathbb{E}[\mathbf{t}_{\text{RAN}} \mathbf{t}_{\text{RAN}}^H] = \frac{1-\beta_r}{N_r-1} \mathbf{I}_{N_r-1}$. According to (6), (7), and (8), we express the received signal at the destination in the second hop transmission as

$$\mathbf{y}_d = \sqrt{P_r d_{rd}^{-\eta}} \mathbf{H}_{rd} (\mathbf{w}_R t_R + \mathbf{W}_{\text{RAN}} \mathbf{t}_{\text{RAN}}) + \mathbf{n}_d, \quad (9)$$

where P_r denotes the transmit power at the relay and \mathbf{n}_d denotes the thermal noise at the destination, the elements of which are assumed to be i.i.d complex random variables with zero mean and variance σ_d^2 , i.e., $\mathbf{n}_d \sim \mathcal{CN}(\mathbf{0}_{N_d}, \sigma_d^2 \mathbf{I}_{N_d})$. We note that AN signals in (9) can also be canceled at the destination by applying MRC.

In order to further confuse the eavesdroppers in the second hop transmission, we assume that the source transmits AN signals using transmit power P_s . We denote the AN signals from the source in the second hop transmission as \mathbf{x}_{AN} , the elements of which follow the i.i.d zero mean complex Gaussian distribution. We assume that \mathbf{x}_{AN} has unit power such that $\mathbb{E}[\mathbf{x}_{\text{AN}} \mathbf{x}_{\text{AN}}^H] = \mathbf{I}_{N_s}/N_s$. We next express the received signal in the second hop transmission at a typical eavesdropper located at i , $i \in \Phi$, as

$$\mathbf{y}_i^{(2)} = \sqrt{P_r d_{ri}^{-\eta}} \mathbf{H}_{ri} (\mathbf{w}_R \mathbf{t}_R + \mathbf{W}_{\text{RAN}} \mathbf{t}_{\text{RAN}}) + \sqrt{P_s d_{si}^{-\eta}} \mathbf{H}_{si} \mathbf{x}_{\text{AN}} + \mathbf{n}_{i2}, \quad (10)$$

where \mathbf{H}_{ri} denotes the $N_e \times N_r$ channel matrix from the relay to the typical eavesdropper located at i , d_{ri} denotes the distance between the relay and the typical eavesdropper located at i , and \mathbf{n}_{i2} denotes the thermal noise vector at a typical eavesdropper located at i , the elements of which are assumed to be i.i.d complex Gaussian random variables with zero mean and variance σ_{i2}^2 , i.e., $\mathbf{n}_{i2} \sim \mathcal{CN}(\mathbf{0}_{N_e}, \sigma_{i2}^2 \mathbf{I}_{N_e})$.

B. Formulation of Received Signal-to-Noise Ratios

We first focus on the equivalent instantaneous SNR at the destination. Recall that both the relay and the destination apply MRC to process received signals. We express the MRC combiner at the relay in the first hop transmission as $\mathbf{v}_r = \frac{\mathbf{w}_S^H \mathbf{H}_{sr}^H}{\|\mathbf{H}_{sr} \mathbf{w}_S\|}$, and express the MRC combiner at the destination in the second hop transmission as $\mathbf{v}_d = \frac{\mathbf{w}_R^H \mathbf{H}_{rd}^H}{\|\mathbf{H}_{rd} \mathbf{w}_R\|}$. Using \mathbf{v}_r and \mathbf{v}_d , we express the instantaneous SNR at the relay in the first hop transmission and the instantaneous SNR at the destination in the second hop transmission as $\gamma_{sr} = \frac{\beta_s P_s}{d_{sr}^\eta \sigma_r^2} \lambda_{\text{max}}^{sr}$ and $\gamma_{rd} = \frac{\beta_r P_r}{d_{rd}^\eta \sigma_d^2} \lambda_{\text{max}}^{rd}$, respectively. As per the rules of the DF protocol, we express the equivalent end-to-end SNR from the source to the destination as [23]

$$\Gamma_D = \min\{\gamma_{sr}, \gamma_{rd}\}. \quad (11)$$

We now focus on the equivalent SNR at the eavesdroppers. In order to maximize the probability of successful eavesdropping, we assume that the eavesdropper utilizes the minimum mean square error (MMSE) combining to process the received signals within two time slots. As per the rules of the MMSE combining, we express the instantaneous SNR at a typical eavesdropper located at i in the first hop transmission and the second hop transmission as

$$\gamma_{si} = \beta_s P_s d_{si}^{-\eta} \mathbf{w}_S^H \mathbf{H}_{si}^H \mathbf{K}_{si}^{-1} \mathbf{H}_{si} \mathbf{w}_S, \quad (12)$$

and

$$\gamma_{ri} = \beta_r P_r d_{ri}^{-\eta} \mathbf{w}_R^H \mathbf{H}_{ri}^H \mathbf{K}_{ri}^{-1} \mathbf{H}_{ri} \mathbf{w}_R, \quad (13)$$

respectively, where

$$\mathbf{K}_{si} = \frac{1 - \beta_s}{N_s - 1} P_s d_{si}^{-\eta} \mathbf{H}_{si} \mathbf{W}_{\text{SAN}} \mathbf{W}_{\text{SAN}}^H \mathbf{H}_{si}^H + \sigma_{i1}^2 \mathbf{I}_{N_e}, \quad (14)$$

and

$$\mathbf{K}_{ri} = \frac{1 - \beta_r}{N_r - 1} P_r d_{ri}^{-\eta} \mathbf{H}_{ri} \mathbf{W}_{\text{RAN}} \mathbf{W}_{\text{RAN}}^H \mathbf{H}_{ri}^H + \frac{P_s}{N_s} d_{si}^{-\eta} \mathbf{H}_{si} \mathbf{H}_{si}^H + \sigma_{i2}^2 \mathbf{I}_{N_e}. \quad (15)$$

We assume that the eavesdroppers are non-colluding, indicating that each eavesdropper decodes her own received signals from the source and the relay without cooperating with other eavesdroppers. We also assume that the source and the relay use different codebooks. As such, the transmitted signals from the source and the transmitted signals from the relay cannot be jointly processed at each eavesdropper. Based on (12) and (13), we express the equivalent SNR at the eavesdroppers as

$$\Gamma_E = \max_{i \in \Phi} \{\max\{\gamma_{si}, \gamma_{ri}\}\}. \quad (16)$$

III. SECRECY PERFORMANCE ANALYSIS

In this section, we analyze the secrecy performance achieved by the transmission scheme detailed in Section II. We first derive a closed-form expression for the transmission outage probability and an easy-to-compute expression for the secrecy outage probability, both of which are valid for an arbitrary number of antennas at the source, relay, and destination. We then derive simple yet valuable expressions for the asymptotic transmission outage probability and the asymptotic secrecy outage probability, both of which are valid for a sufficiently large number of antennas at the source, i.e., $N_s \rightarrow \infty$. We further describe in detail how the secrecy throughput of the relay wiretap channel is quantified and how the maximum secrecy throughput is obtained under a secrecy outage probability constraint.

A. Preliminaries

In this subsection, we present the statistics of γ_{sr} , γ_{rd} , γ_{si} , and γ_{ri} , which will be used to derive the outage probabilities. We first focus on the cumulative distribution functions (CDFs) of γ_{sr} and γ_{rd} . To this end, we introduce several new notations as follows: $u_1 = \min(N_s, N_r)$, $v_1 = \max(N_s, N_r)$, $t_1 = v_1 - u_1$, $u_2 = \min(N_r, N_d)$, $v_2 = \max(N_r, N_d)$, and $t_2 = v_2 - u_2$. We then obtain the CDF of γ_{sr} as [38]

$$F_{\gamma_{sr}}(\gamma) = \frac{\det\left(\Xi\left(\frac{\gamma}{\beta_s \gamma_{sr}}\right)\right)}{\Gamma_{u_1}(u_1) \Gamma_{v_1}(u_1)}, \quad (17)$$

where $\Xi\left(\frac{\gamma}{\beta_s \gamma_{sr}}\right)$ is a $u_1 \times u_1$ matrix with (i, j) th entry, $\xi_{ij}\left(\frac{\gamma}{\beta_s \gamma_{sr}}\right)$, given by

$$\xi_{ij}\left(\frac{\gamma}{\beta_s \gamma_{sr}}\right) = \gamma \left(g_1(i, j), \frac{\gamma}{\beta_s \gamma_{sr}}\right). \quad (18)$$

In (18), $\gamma(\cdot)$ denotes the incomplete gamma function, defined as [39, Eq. (8.352)]

$$\gamma(k, x) = \Gamma(k) \left(1 - \exp(-x) \sum_{z=0}^{k-1} \frac{x^z}{z!}\right) \quad (19)$$

for integer k , where $\Gamma(\cdot)$ denotes the gamma function, defined as $\Gamma(k) = (k-1)!$ for integer k [39, Eq. (8.339)], $g_1(i, j) = t_1 + i + j - 1$, $\bar{\gamma}_{sr} = P_s d_{sr}^{-\eta} \sigma_r^{-2}$, and

$$\Gamma_m(n) = \prod_{i=1}^n \Gamma(m-i+1). \quad (20)$$

Similarly, we obtain the CDF of γ_{rd} as

$$F_{\gamma_{rd}}(\gamma) = \frac{\det\left(\Theta\left(\frac{\gamma}{\beta_r \bar{\gamma}_{rd}}\right)\right)}{\Gamma_{u_2}(u_2) \Gamma_{v_2}(u_2)}, \quad (21)$$

where $\Theta\left(\frac{\gamma}{\beta_r \bar{\gamma}_{rd}}\right)$ is a $u_2 \times u_2$ matrix with (i, j) th entry, $\theta_{ij}\left(\frac{\gamma}{\beta_r \bar{\gamma}_{rd}}\right)$, given by

$$\theta_{ij}\left(\frac{\gamma}{\beta_r \bar{\gamma}_{rd}}\right) = \gamma \left(g_2(i, j), \frac{\gamma}{\beta_r \bar{\gamma}_{rd}}\right), \quad (22)$$

where $g_2(i, j) = t_2 + i + j - 1$, and $\bar{\gamma}_{rd} = P_r d_{rd}^{-\eta} \sigma_d^{-2}$.

With the aid of [40], we express the CDF of γ_{si} as

$$\begin{aligned} F_{\gamma_{si}}(\gamma) &= 1 - \frac{\exp\left(-\frac{\gamma}{\beta_s \bar{\gamma}_{si}}\right)}{(1 + \kappa_1 \gamma)^{N_s-1}} \sum_{p=1}^{N_e} \frac{1}{\Gamma(p)} \left(\frac{\gamma}{\beta_s \bar{\gamma}_{si}}\right)^{p-1} \\ &\quad \times \sum_{q=0}^{N_e-p} \binom{N_s-1}{q} (\kappa_1 \gamma)^q \end{aligned} \quad (23)$$

where $\bar{\gamma}_{si} = P_s d_{si}^{-\eta} \sigma_{i1}^{-2}$ and $\kappa_1 = \frac{1 - \beta_s}{\beta_s (N_s - 1)}$, and express the CDF of γ_{ri} as

$$\begin{aligned} F_{\gamma_{ri}}(\gamma) &= 1 - \frac{\exp\left(-\frac{\gamma}{\beta_r \bar{\gamma}_{ri}}\right)}{(1 + \kappa_2 \gamma)^{N_r-1} (1 + \kappa_3 \gamma)^{N_s}} \sum_{m=1}^{N_e} \frac{1}{\Gamma(m)} \left(\frac{\gamma}{\beta_r \bar{\gamma}_{ri}}\right)^{m-1} \\ &\quad \times \sum_{n=0}^{N_e-m} \binom{N_r-1}{n} (\kappa_2 \gamma)^n \sum_{l=0}^{N_e-m-n} \binom{N_s}{l} (\kappa_3 \gamma)^l, \end{aligned} \quad (24)$$

where $\bar{\gamma}_{ri} = P_r d_{ri}^{-\eta} \sigma_{i2}^{-2}$, $\kappa_2 = \frac{1 - \beta_r}{\beta_r (N_r - 1)}$, and $\kappa_3 = \frac{P_s d_{ri}^{\eta}}{\beta_r P_r N_s d_{si}^{\eta}}$.

B. Outage Probabilities

In this subsection, we define the transmission outage event and the secrecy outage event and then characterize their probabilities. We first denote C_b as the instantaneous capacity between the source and the destination. According to (11), C_b is given by

$$C_b = \frac{1}{2} \log_2(1 + \Gamma_D), \quad (25)$$

where the presence of the factor $1/2$ is due to the fact that two time slots are used in the transmission. We also denote C_e as the instantaneous capacity between the source and the eavesdropper. According to (16), C_e is given by

$$C_e = \frac{1}{2} \log_2(1 + \Gamma_E). \quad (26)$$

We assume that the wiretap code is adopted in the transmission. We denote (R_b, R_e) as the parameter pair for the adopted wiretap code, where R_b denotes the transmission rate

of the wiretap code, and R_e denotes the redundancy rate of the wiretap code revealing the cost of preventing eavesdropping. We also assume that the source and the relay use the same (R_b, R_e) to transmit, but with different codebooks. As such, we define that the transmission outage event occurs when $C_b < R_b$. In this event, the received signals at the destination are not reliably decoded. We also define that the secrecy outage event occurs when $C_e \geq R_e$. In this event, the eavesdropper is able to decode the transmitted signals and secrecy is compromised.

Based on the definition of the transmission outage event, we define the transmission outage probability as the probability that the equivalent instantaneous SNR at the destination is less than $\tau_b = 2^{R_b} - 1$. Mathematically, P_{to} is formulated as

$$P_{to} = \Pr(\Gamma_D < \tau_b). \quad (27)$$

Using (11), (17), and (21), we re-express the transmission outage probability in (27) as

$$\begin{aligned} P_{to} &= \Pr(\min\{\gamma_{sr}, \gamma_{rd}\} < \tau_b) \\ &= 1 - (1 - F_{\gamma_{sr}}(\tau_b))(1 - F_{\gamma_{rd}}(\tau_b)) \\ &= \frac{\det\left(\Xi\left(\frac{\tau_b}{\beta_s \bar{\gamma}_{sr}}\right)\right)}{\Gamma_{u_1}(u_1) \Gamma_{v_1}(u_1)} + \frac{\det\left(\Theta\left(\frac{\tau_b}{\beta_r \bar{\gamma}_{rd}}\right)\right)}{\Gamma_{u_2}(u_2) \Gamma_{v_2}(u_2)} \\ &\quad - \frac{\det\left(\Xi\left(\frac{\tau_b}{\beta_s \bar{\gamma}_{sr}}\right)\right) \det\left(\Theta\left(\frac{\tau_b}{\beta_r \bar{\gamma}_{rd}}\right)\right)}{\Gamma_{u_1}(u_1) \Gamma_{v_1}(u_1) \Gamma_{u_2}(u_2) \Gamma_{v_2}(u_2)}. \end{aligned} \quad (28)$$

Based on the definition of the secrecy outage event, we define the secrecy outage probability as the probability that Γ_E is larger than $\tau_e = 2^{R_e} - 1$. Mathematically, P_{so} is formulated as

$$P_{so} = \Pr(\Gamma_E > \tau_e). \quad (29)$$

According to (16), (23), and (24), we derive an easy-to-compute expression for the secrecy outage probability in the following theorem.

Theorem 1: The secrecy outage probability of the relay wiretap channel is derived as

$$P_{so} = 1 - \exp(-2\lambda(\mathcal{J}_1 + \mathcal{J}_2 - \mathcal{J}_3)), \quad (30)$$

where

$$\begin{aligned} \mathcal{J}_1 &= \frac{\pi}{\eta} \left(\frac{\beta_s P_s}{\tau_e \sigma_{i1}^2}\right)^{\frac{2}{\eta}} (1 + \kappa_1 \tau_e)^{-(N_s-1)} \\ &\quad \times \sum_{p=1}^{N_e} \frac{\Gamma\left(\frac{2}{\eta} + p - 1\right)}{\Gamma(p)} \sum_{q=0}^{N_e-p} \binom{N_s-1}{q} (\kappa_1 \tau_e)^q, \end{aligned} \quad (31)$$

\mathcal{J}_2 and \mathcal{J}_3 are given by (32) and (33), respectively, shown at the top of the next page. In (32) and (33), we have $\psi(\theta) = \frac{\tau_e \sigma_{i2}^2}{\beta_r P_r} (d_{sr}^2 + d_{si}^2 - 2d_{sr}d_{si}\cos\theta)^{\frac{\eta}{2}}$.

Proof: See Appendix A. ■

We find that *Theorem 1* provides an easy-to-compute tool for efficiently evaluating the secrecy outage probability. Although \mathcal{J}_2 and \mathcal{J}_3 for general η cannot be obtained in closed-form, they can be easily calculated since only a double integral is involved in \mathcal{J}_2 and \mathcal{J}_3 .

$$\begin{aligned} \mathcal{J}_2 = & (1 + \kappa_2 \tau_e)^{-(N_r-1)} \int_0^\infty \int_0^\pi d_{si} \frac{\exp(-\psi(\theta))}{\left(1 + \frac{P_s \psi(\theta)}{N_s d_{si}^\eta \sigma_{i2}^2}\right)^{N_s}} \sum_{m=1}^{N_e} \frac{1}{\Gamma(m)} (\psi(\theta))^{m-1} \\ & \times \sum_{n=0}^{N_e-m} \binom{N_r-1}{n} (\kappa_2 \tau_e)^n \sum_{l=0}^{N_e-m-n} \binom{N_s}{l} \left(\frac{P_s \psi(\theta)}{N_s d_{si}^\eta \sigma_{i2}^2}\right)^l dd_{si} d\theta, \end{aligned} \quad (32)$$

$$\begin{aligned} \mathcal{J}_3 = & (1 + \kappa_1 \tau_e)^{-(N_s-1)} (1 + \kappa_2 \tau_e)^{-(N_r-1)} \int_0^\infty \int_0^\pi d_{si} \exp\left(-\frac{\tau_e \sigma_{i1}^2}{\beta_s P_s} d_{si}^\eta\right) \sum_{p=1}^{N_e} \frac{1}{\Gamma(p)} \left(\frac{\tau_e \sigma_{i1}^2}{\beta_s P_s} d_{si}^\eta\right)^{p-1} \sum_{q=0}^{N_e-p} \binom{N_s-1}{q} (\kappa_1 \tau_e)^q \\ & \times \frac{\exp(-\psi(\theta))}{\left(1 + \frac{P_s \psi(\theta)}{N_s d_{si}^\eta \sigma_{i2}^2}\right)^{N_s}} \sum_{m=1}^{N_e} \frac{1}{\Gamma(m)} (\psi(\theta))^{m-1} \sum_{n=0}^{N_e-m} \binom{N_r-1}{n} (\kappa_2 \tau_e)^n \sum_{l=0}^{N_e-m-n} \binom{N_s}{l} \left(\frac{P_s \psi(\theta)}{N_s d_{si}^\eta \sigma_{i2}^2}\right)^l dd_{si} d\theta. \end{aligned} \quad (33)$$

C. Asymptotic Outage Probabilities

In this subsection, we examine the asymptotic behavior of the outage probabilities as $N_s \rightarrow \infty$. The obtained asymptotic results are particularly valuable for large-scale MIMO systems where the source (or equivalently, the BS) is equipped with a sufficiently large number of antennas. We first present the expression for the asymptotic transmission outage probability in the following corollary.

Corollary 1: The asymptotic transmission outage probability when $N_s \rightarrow \infty$ is given by

$$P_{to}^\infty = \frac{\det\left(\Theta\left(\frac{\tau_b}{\beta_r \gamma_{rd}}\right)\right)}{\Gamma_{u_2}(u_2) \Gamma_{v_2}(u_2)}. \quad (34)$$

Proof: We express the asymptotic transmission outage probability when $N_s \rightarrow \infty$ as

$$P_{to}^\infty = \lim_{N_s \rightarrow \infty} P_{to}. \quad (35)$$

We note that

$$\lim_{N_s \rightarrow \infty} \frac{\Xi\left(\frac{\tau_b}{\beta_s \gamma_{sr}}\right)}{\Gamma_{u_1}(u_1) \Gamma_{v_1}(u_1)} = 0. \quad (36)$$

Substituting (36) into (35) yields the result. ■

According to *Corollary 1*, we find that the asymptotic transmission outage probability is solely determined by γ_{rd} when $N_s \rightarrow \infty$. This finding is due to the fact that $\gamma_{sr} \rightarrow \infty$ when $N_s \rightarrow \infty$. As such, we conclude that the probability that Γ_D is less than τ_b when $N_s \rightarrow \infty$ is determined by the link quality of the relay-destination channel only.

We next present the asymptotic secrecy outage probability when $N_s \rightarrow \infty$ in the following corollary.

Corollary 2: The asymptotic secrecy outage probability when $N_s \rightarrow \infty$ is given by

$$P_{so}^\infty = 1 - \exp(-2\lambda(\mathcal{J}_1^\infty + \mathcal{J}_2^\infty - \mathcal{J}_3^\infty)), \quad (37)$$

where

$$\begin{aligned} \mathcal{J}_1^\infty = & \frac{\pi}{\eta} \left(\frac{\beta_s P_s}{\tau_e \sigma_{i1}^2}\right)^{\frac{2}{\eta}} \exp\left(-\frac{1-\beta_s}{\beta_s} \tau_e\right) \\ & \times \sum_{p=1}^{N_e} \frac{\Gamma\left(\frac{2}{\eta} + p - 1\right)}{\Gamma(p)} \sum_{q=0}^{N_e-p} \frac{\left(\frac{1-\beta_s}{\beta_s} \tau_e\right)^q}{\Gamma(q+1)}, \end{aligned} \quad (38)$$

\mathcal{J}_2^∞ and \mathcal{J}_3^∞ are given by (39) and (40), respectively, shown at the top of the next page.

Proof: We express the asymptotic secrecy outage probability when $N_s \rightarrow \infty$ as

$$P_{so}^\infty = \lim_{N_s \rightarrow \infty} P_{so}. \quad (41)$$

We note that

$$\lim_{N_s \rightarrow \infty} \left(1 + \frac{(1-\beta_s)\tau_e}{\beta_s(N_s-1)}\right)^{-(N_s-1)} = \exp\left(-\frac{1-\beta_s}{\beta_s} \tau_e\right), \quad (42)$$

and

$$\lim_{N_s \rightarrow \infty} \binom{N_s-1}{q} \left(\frac{(1-\beta_s)\tau_e}{\beta_s(N_s-1)}\right)^q = \frac{\left(\frac{1-\beta_s}{\beta_s} \tau_e\right)^q}{\Gamma(q+1)}. \quad (43)$$

We also note

$$\lim_{N_s \rightarrow \infty} \left(1 + \frac{P_s \psi(\theta)}{N_s d_{si}^\eta \sigma_{i2}^2}\right)^{-N_s} = \exp\left(-\frac{P_s \psi(\theta)}{d_{si}^\eta \sigma_{i2}^2}\right), \quad (44)$$

and

$$\lim_{N_s \rightarrow \infty} \binom{N_s}{l} \left(\frac{P_s \psi(\theta)}{N_s d_{si}^\eta \sigma_{i2}^2}\right)^l = \frac{\left(\frac{P_s \psi(\theta)}{d_{si}^\eta \sigma_{i2}^2}\right)^l}{\Gamma(l+1)}. \quad (45)$$

Substituting (42), (43), (44), and (45) into (41) yields (37), which completes the proof. ■

According to *Corollary 2*, we find that the asymptotic secrecy outage probability approaches a certain value that is independent of N_s when $N_s \rightarrow \infty$. This reveals that adding extra transmit antennas at the source does not always decrease the secrecy outage probability.

D. Secrecy Throughput

So far, we have derived the exact and the asymptotic transmission outage probability and secrecy outage probability of the considered relay wiretap channel. Our derived expressions are valid for given R_b , R_e , β_s , and β_r . A question then naturally arises: “How do we determine the optimal $(R_b^*, R_e^*, \beta_s^*, \beta_r^*)$ that achieves the maximum secrecy performance of this relay wiretap channel, under a secrecy outage probability constraint?” Our answer to this question

$$\begin{aligned} \mathcal{J}_2^\infty &= (1 + \kappa_2 \tau_e)^{-(N_r-1)} \int_0^\infty \int_0^\pi d_{si} \exp \left(-\psi(\theta) - \frac{P_s \psi(\theta)}{d_{si}^\eta \sigma_{i2}^2} \right) \sum_{m=1}^{N_e} \frac{1}{\Gamma(m)} (\psi(\theta))^{m-1} \\ &\quad \times \sum_{n=0}^{N_e-m} \binom{N_r-1}{n} (\kappa_2 \tau_e)^n \sum_{l=0}^{N_e-m-n} \frac{\left(\frac{P_s \psi(\theta)}{d_{si}^\eta \sigma_{i2}^2} \right)^l}{\Gamma(l+1)} dd_{si} d\theta, \end{aligned} \quad (39)$$

$$\begin{aligned} \mathcal{J}_3^\infty &= \frac{\exp \left(-\frac{1-\beta_s \tau_e}{\beta_s} \right)}{(1 + \kappa_2 \tau_e)^{N_r-1}} \int_0^\infty \int_0^\pi d_{si} \exp \left(-\frac{\tau_e \sigma_{i1}^2}{\beta_s P_s} d_{si}^\eta \right) \sum_{p=1}^{N_e} \frac{1}{\Gamma(p)} \left(\frac{\tau_e \sigma_{i1}^2}{\beta_s P_s} d_{si}^\eta \right)^{p-1} \sum_{q=0}^{N_e-p} \frac{\left(\frac{1-\beta_s \tau_e}{\beta_s} \right)^q}{\Gamma(q+1)} \\ &\quad \times \exp \left(-\psi(\theta) - \frac{P_s \psi(\theta)}{d_{si}^\eta \sigma_{i2}^2} \right) \sum_{m=1}^{N_e} \frac{1}{\Gamma(m)} (\psi(\theta))^{m-1} \sum_{n=0}^{N_e-m} \binom{N_r-1}{n} (\kappa_2 \tau_e)^n \sum_{l=0}^{N_e-m-n} \frac{\left(\frac{P_s \psi(\theta)}{d_{si}^\eta \sigma_{i2}^2} \right)^l}{\Gamma(l+1)} dd_{si} d\theta. \end{aligned} \quad (40)$$

demonstrates the usefulness of our analytical expressions in a wider sense. It shows how the expressions can be embedded and utilized in a complex optimization problem, presenting a solution that can be determined in a much faster manner than would otherwise be possible. A concrete example of this usefulness in an operational sense, would be the dynamic and real-time determination of the optimal system parameter settings for a given secrecy performance metric.

To answer the question, we utilize our derived expressions directly to characterize the secrecy performance of the relay wiretap channel. As a specific example, we consider the metric termed the *secrecy throughput* introduced by [10]. This performance metric quantifies the average confidential information rate when the source transmits. The secrecy throughput for the relay wiretap channel is given by

$$T_s = (R_b - R_e)(1 - P_{to}). \quad (46)$$

The maximization problem is accordingly formulated as

$$\max_{R_b, R_e, \beta_s, \beta_r} T_s, \quad (47a)$$

$$s.t. \quad P_{so} \leq \varphi, \quad (47b)$$

$$0 \leq R_e \leq R_b, \quad (47c)$$

$$0 < \beta_s \leq 1, 0 < \beta_r \leq 1. \quad (47d)$$

In the following, we describe in detail how the maximum secrecy throughput is obtained by judiciously selecting the transmission parameters². To this end, we solve the maximization problem in (47) in two steps. First, we fix power allocation factors β_s and β_r , and choose the wiretap code rates pair, (R_b^*, R_e^*) , that maximizes the secrecy throughput. Accordingly, the maximum secrecy throughput achieved by (R_b^*, R_e^*) for given β_s and β_r is defined as T_s^* . Second, we choose the wiretap code rates as well as the power allocation factor, $(R_b^{*\circ}, R_e^{*\circ}, \beta_s^{*\circ}, \beta_r^{*\circ})$, that jointly maximizes T_s . The details of these two steps are presented as follows:

1) (R_b^*, R_e^*) for given β_s and β_r : The wiretap code rates pair, (R_b^*, R_e^*) , that maximizes T_s for given β_s and β_r is

determined as

$$(R_b^*, R_e^*) = \operatorname{argmax} T_s, \quad (48a)$$

$$s.t. \quad P_{so} \leq \varphi, \quad (48b)$$

$$0 \leq R_e \leq R_b. \quad (48c)$$

Taking the first-order derivative of P_{so} with respect to R_e , we confirm that $\partial P_{so} / \partial R_e < 0$, which indicates that P_{so} monotonically decreases as R_e increases. As such, the value of R_e^* satisfying (48b) is the value of R_e^* that satisfies the secrecy outage probability constraint, i.e., $P_{so}(R_e^*) = \varphi$. We then confirm that $\partial P_{to} / \partial R_b > 0$, which shows that P_{to} monotonically increases as R_e increases. As such, we note that $T_s \rightarrow 0$ as R_b increases such that $P_{to} \rightarrow 1$. Defining R_b^{\max} as the value of R_b that satisfies $P_{to}(R_b) = 1$, we rewrite (48) as

$$(R_b^*, R_e^*) = \operatorname{argmax} T_s, \quad (49a)$$

$$s.t. \quad P_{so} \leq \varphi, \quad (49b)$$

$$R_e^* \leq R_b \leq R_b^{\max}. \quad (49c)$$

Although a closed-form solution for (R_b^*, R_e^*) is mathematically intractable, we are able to find the values of (R_b^*, R_e^*) in a numerical way.

2) $(R_b^{*\circ}, R_e^{*\circ}, \beta_s^{*\circ}, \beta_r^{*\circ})$: The wiretap code rates and power allocation factors which jointly maximizes T_s in (46), $(R_b^{*\circ}, R_e^{*\circ}, \beta_s^{*\circ}, \beta_r^{*\circ})$, is determined as

$$(R_b^{*\circ}, R_e^{*\circ}, \beta_s^{*\circ}, \beta_r^{*\circ}) = \operatorname{argmax} T_s, \quad (50a)$$

$$s.t. \quad P_{so} \leq \varphi, \quad (50b)$$

$$0 \leq R_e \leq R_b, \quad (50c)$$

$$0 < \beta_s \leq 1, 0 < \beta_r \leq 1. \quad (50d)$$

Using (28) and (30), we are able to solve (50) numerically. Specifically, we first select the value of (R_b^*, R_e^*) satisfying (49) for each value of β_s and β_r . This leads to the secrecy throughput with (R_b^*, R_e^*) , denoted by $T_s^* = (R_b^* - R_e^*)(1 - P_{to})$. We then select the value of $\beta_s^{*\circ}$ and the value of $\beta_r^{*\circ}$ that maximize T_s^* for $0 < \beta_s \leq 1$ and $0 < \beta_r \leq 1$. Accordingly, the value of (R_b^*, R_e^*) associated with $\beta_s^{*\circ}$ and $\beta_r^{*\circ}$ is defined as $(R_b^{*\circ}, R_e^{*\circ})$. Finally, the maximum secrecy throughput achieved by $(R_b^{*\circ}, R_e^{*\circ}, \beta_s^{*\circ}, \beta_r^{*\circ})$ is defined as $T_s^{*\circ}$.

²We note that the maximum secrecy throughput is formally a local maximum, since we numerically search the transmission parameters that jointly maximize the secrecy throughput only within anticipated ranges.

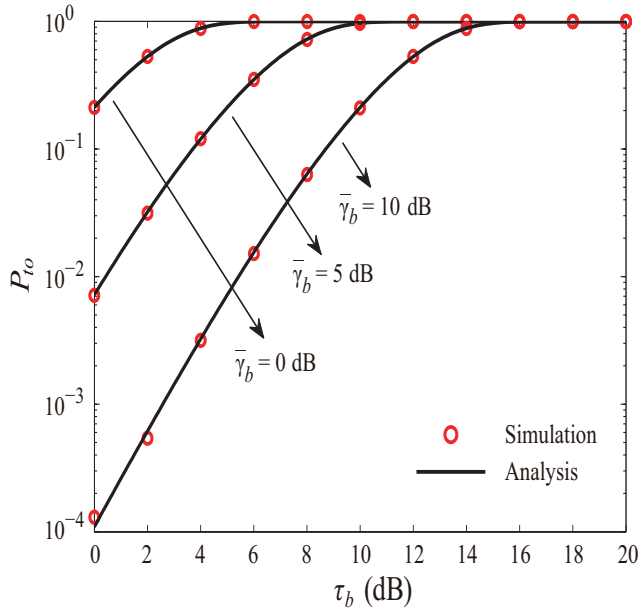


Fig. 2. P_{to} versus τ_b for different values of $\bar{\gamma}_b$ with $\eta = 4$, $N_s = 4$, $N_r = 2$, $N_d = 2$, $N_e = 2$, $\beta_s = \beta_r = 0.5$, $\lambda = 0.01$, and $d_{sr} = d_{rd} = 10$.

We note that our expressions for the outage probabilities can also be implemented in other performance metrics. For example, we can utilize our expressions to characterize the average secrecy rate of the relay wiretap channels in the presence of spatially random eavesdroppers.

IV. NUMERICAL RESULTS

In this section, we present numerical results to validate our analysis of the outage probabilities. We also examine the impact of transmission parameters (e.g., R_b , β_s , β_r) and system parameters (e.g., N_s and λ) on the secrecy throughput of the relay wiretap channel. Throughout this section we concentrate on the practical example of a highly shadowed urban area with $\eta = 4$.

We first demonstrate the accuracy of the transmission outage probability and the secrecy outage probability using Monte Carlo simulations. In Fig. 2, we plot P_{to} versus τ_b for different values of $\bar{\gamma}_b$ with $N_s = 4$, $N_r = 2$, $N_d = 2$, $N_e = 2$, $\beta_s = \beta_r = 0.5$, $\lambda = 0.01$, and $d_{sr} = d_{rd} = 10$. In this figure, we consider $\bar{\gamma}_{sr} = \bar{\gamma}_{rd} = \bar{\gamma}_b$. We first see that the analytical curves, generated from (28), precisely match the simulation points marked by red circles, which demonstrates the correctness of our expression for P_{to} in (28). Second, we see that P_{to} increases monotonically as τ_b increases for a given $\bar{\gamma}_b$. This reveals that the transmission outage probability increases when the transmission rate of the wiretap code increases. We further see that P_{to} decreases as $\bar{\gamma}_b$ increases for a given τ_b . This reveals that the transmission outage probability reduces when the source and the relay use a higher power to transmit for a fixed τ_b .

In Fig. 3, we plot P_{so} versus τ_e for different values of $\bar{\gamma}_e$ with $N_s = 4$, $N_r = 2$, $N_d = 2$, $N_e = 2$, and $\beta_s = \beta_r = 0.5$. In this figure we consider $\bar{\gamma}_{sr}\sigma_r^2/\sigma_{i1}^2 = \bar{\gamma}_{rd}\sigma_d^2/\sigma_{i2}^2 = \bar{\gamma}_e$. We see an excellent match between the analytical curves

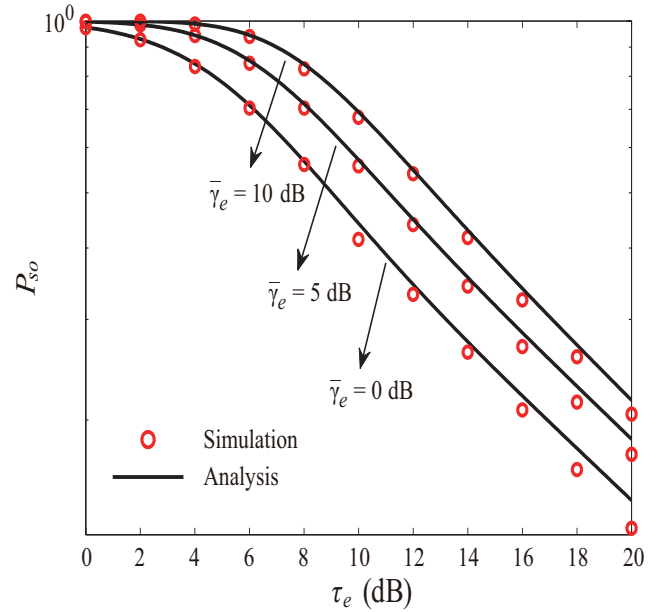


Fig. 3. P_{so} versus τ_e for different values of $\bar{\gamma}_e$ with $\eta = 4$, $N_s = 4$, $N_r = 2$, $N_d = 2$, $N_e = 2$, $\beta_s = \beta_r = 0.5$, $\lambda = 0.01$, and $d_{sr} = d_{rd} = 10$.

generated from (30) and the simulation points marked by red circles, demonstrating the correctness of our expression for P_{so} in (30). We then see that P_{so} decreases monotonically as τ_e increases for a given $\bar{\gamma}_e$, which shows that the secrecy outage probability decreases when the redundancy rate of the wiretap code increases. We further observe that P_{so} increases as $\bar{\gamma}_e$ increases. This is due to the fact the eavesdroppers receive signals from *both* the source and the relay. It follows that increasing the transmit power at the source and the relay leads to an improved received SNR at the eavesdroppers.

In the following, we examine the impact of the transmission parameters on the secrecy throughput that is characterized by the derived outage probabilities. We first examine the impact of R_b on T_s . In Fig. 4, we plot T_s versus R_b for different values of N_s with R_e^* and fixed N_d , N_e , β_s , and β_r . We first observe that there exists a unique R_b^* that maximizes T_s for given β_s and β_r . We also observe that the maximum T_s for given β_s and β_r , i.e., T_s^* , increases as N_s increases. This shows that adding extra transmit antennas at the source significantly enhances the secrecy performance of the relay wiretap channel.

We next examine the impact of β_s and β_r on T_s^* . In Fig. 5, we plot T_s^* versus β_s for different values of N_s with a fixed β_r . For each point of T_s^* , we choose (R_b^*, R_e^*) that maximizes T_s for the corresponding β_s . We first observe that there exists a unique β_s^{*o} that maximizes T_s^* . We then observe that the maximum T_s^* for a fixed β_r increases as N_s increases. Furthermore, we observe that the value of β_s^{*o} slightly decreases as N_s increases, which shows that in order to maintain the maximum secrecy throughput, the power allocated to AN signals at the source needs to be increased as the number of antennas at the source increases.

In Fig. 6, we plot T_s^* versus β_r for different values of N_s with a fixed β_s . Similar as Fig. 5, for each point of T_s^* , we choose (R_b^*, R_e^*) that maximizes T_s for the corresponding β_r .

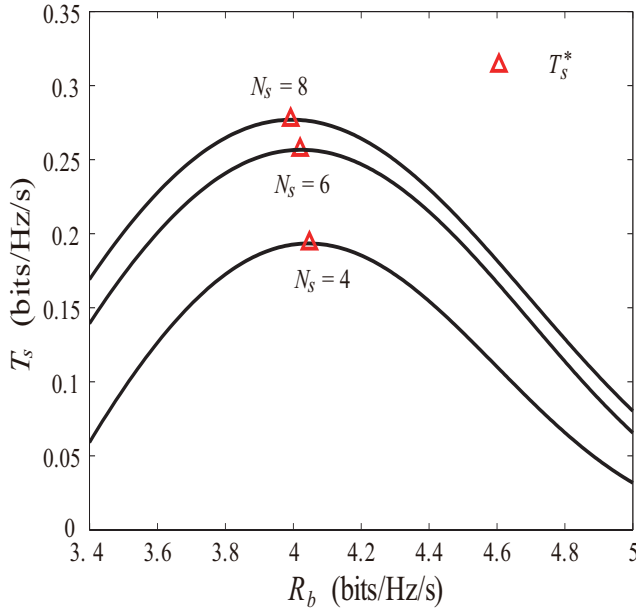


Fig. 4. T_s versus R_b for different values of N_s with $\eta = 4$, $N_r = 2$, $N_d = 2$, $N_e = 2$, $\beta_s = \beta_r = 0.5$, $\lambda = 0.01$, $d_{sr} = d_{rd} = 10$, $\varphi = 0.4$, $\bar{\gamma}_b = 10$ dB, and $\bar{\gamma}_b/\bar{\gamma}_e = 20$.

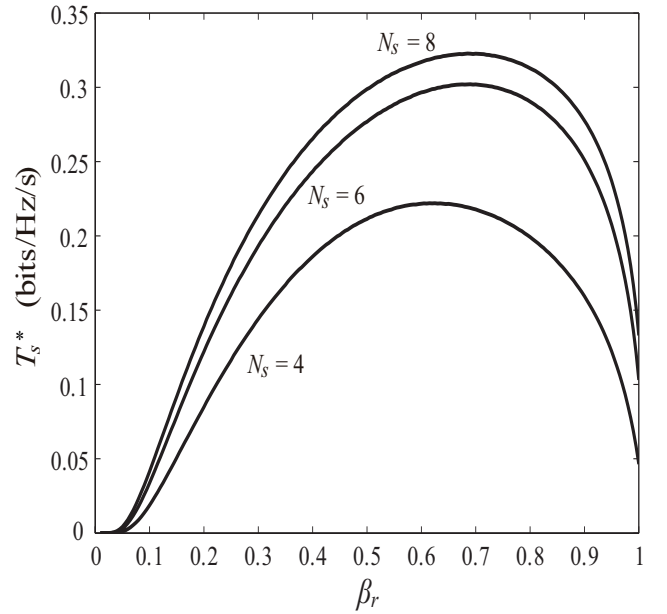


Fig. 6. T_s^* versus β_r for different values of N_s with $\eta = 4$, $N_r = 2$, $N_d = 2$, $N_e = 2$, $\beta_s = 0.5$, $\lambda = 0.01$, $d_{sr} = d_{rd} = 10$, $\varphi = 0.4$, $\bar{\gamma}_b = 10$ dB, and $\bar{\gamma}_b/\bar{\gamma}_e = 20$.

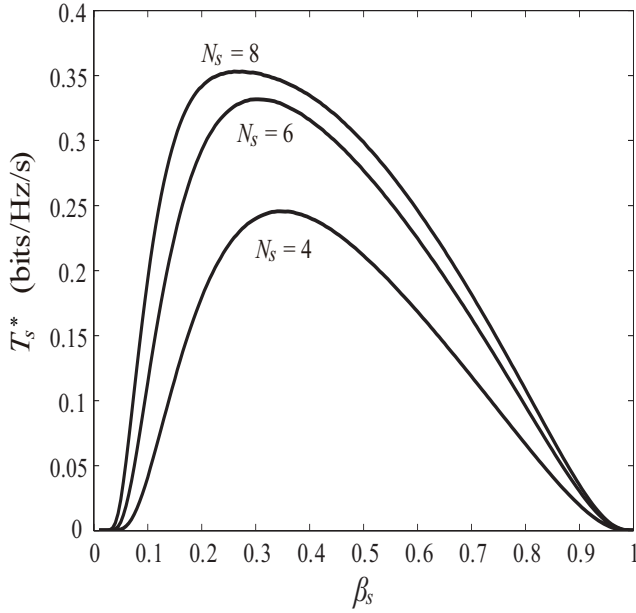


Fig. 5. T_s^* versus β_s for different values of N_s with $\eta = 4$, $N_r = 2$, $N_d = 2$, $N_e = 2$, $\beta_r = 0.5$, $\lambda = 0.01$, $d_{sr} = d_{rd} = 10$, $\varphi = 0.4$, $\bar{\gamma}_b = 10$ dB, and $\bar{\gamma}_b/\bar{\gamma}_e = 20$.

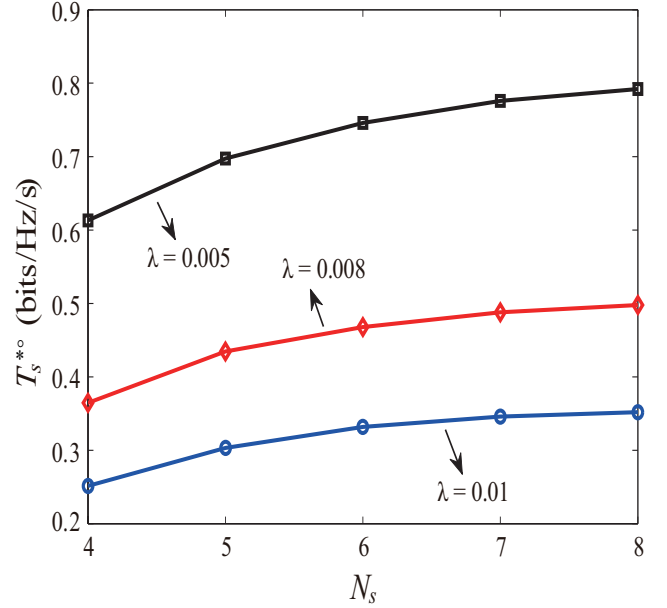


Fig. 7. T_s^{*o} versus N_s for different values of λ with $\eta = 4$, $N_r = 2$, $N_d = 2$, $N_e = 2$, $d_{sr} = d_{rd} = 10$, $\varphi = 0.4$, $\bar{\gamma}_b = 10$ dB, and $\bar{\gamma}_b/\bar{\gamma}_e = 20$.

First, we see a unique β_r^{*o} that maximizes T_s^* . Second, we see that the maximum T_s^* for a fixed β_s increases as N_s increases. Additionally, we note that the value of β_r^{*o} increases as N_s increases, demonstrating that a lower power is needed to be allocated to AN signals at the relay in order to achieve the maximum secrecy throughput when the antenna number at the source increases.

Finally, we examine the impact of N_s and λ on T_s^{*o} . In Fig. 7, we plot T_s^{*o} versus N_s for different values of λ . For each point of T_s^{*o} , we choose $(\beta_s^{*o}, \beta_r, R_b^{*o}, R_e^{*o})$ that maximizes

T_s . We first observe that T_s^{*o} increases as N_s increases. This observation is consistent with the observation in Fig. 4. We then observe that T_s^{*o} decreases as λ increases. This is due to the fact that more eavesdroppers exist as λ increases. The increasing number of eavesdroppers increases the value of R_e^* that satisfies the secrecy constraint.

V. CONCLUSION

We designed the secure transmission that maximizes the secrecy throughput of the generalized relay wiretap channel in

the presence of spatially random multi-antenna eavesdroppers. In the transmission we assumed that both the source and the relay transmit AN signals with information signals in order to confuse the eavesdroppers. Considering the use of the decode-and-forward relaying protocol, we first derived a closed-form expression for the transmission outage probability and an easy-to-compute expression for the secrecy outage probability. We then derived simple yet valuable expressions for the asymptotic transmission outage probability and the asymptotic secrecy outage probability when the number of antennas at the source becomes sufficiently large. Using our derived expressions, we characterized the secrecy throughput of the the relay wiretap channel and then determined the transmission and system parameters that achieve the maximum secrecy throughput. Finally, we evaluated the impact of these parameters on the secrecy throughput.

APPENDIX A PROOF OF THEOREM 1

According to (16), (23), and (24), we re-express (29) as

$$\begin{aligned}
 P_{so} &= 1 - \Pr \{ \Gamma_E \leq \tau_e \} \\
 &= 1 - \Pr \left\{ \max_{i \in \Phi} \{ \max \{ \gamma_{si}, \gamma_{ri} \} \} \leq \tau_e \right\} \\
 &= 1 - \mathbb{E}_\Phi \left[\prod_{i \in \Phi} \Pr \{ \max \{ \gamma_{si}, \gamma_{ri} \} \leq \tau_e \} \right] \\
 &= 1 - \mathbb{E}_\Phi \left[\prod_{i \in \Phi} F_{\gamma_{si}}(\tau_e) F_{\gamma_{ri}}(\tau_e) \right] \\
 &\stackrel{(a)}{=} 1 - \exp(-2\lambda(\mathcal{J}_1 + \mathcal{J}_2 - \mathcal{J}_3)). \quad (48)
 \end{aligned}$$

where

$$\begin{aligned}
 \mathcal{J}_1 &= \int_0^\infty \int_0^\pi d_{si} \left(\frac{\exp\left(-\frac{\tau_e \sigma_{i1}^2 d_{si}^\eta}{\beta_s P_s}\right)}{(1 + \kappa_1 \tau_e)^{N_s-1}} \sum_{p=1}^{N_e} \frac{1}{\Gamma(p)} \left(\frac{\tau_e \sigma_{i1}^2 d_{si}^\eta}{\beta_s P_s} \right)^{p-1} \right. \\
 &\quad \times \sum_{q=0}^{N_e-p} \binom{N_s-1}{q} (\kappa_1 \tau_e)^q \left. \right) dd_{si} d\theta, \quad (49)
 \end{aligned}$$

$$\begin{aligned}
 \mathcal{J}_2 &= \int_0^\infty \int_0^\pi d_{si} \frac{\exp\left(-\frac{\tau_e \sigma_{i2}^2 d_{ri}^\eta}{\beta_r P_r}\right)}{(1 + \kappa_2 \tau_e)^{N_r-1} \left(1 + \frac{P_s \tau_e d_{ri}^\eta}{\beta_r P_r N_s d_{si}^\eta}\right)^{N_s}} \\
 &\quad \times \sum_{m=1}^{N_e} \frac{1}{\Gamma(m)} \left(\frac{\tau_e \sigma_{i2}^2 d_{ri}^\eta}{\beta_r P_r} \right)^{m-1} \sum_{n=0}^{N_e-m} \binom{N_r-1}{n} (\kappa_2 \tau_e)^n \\
 &\quad \times \sum_{l=0}^{N_e-m-n} \binom{N_s}{l} \left(\frac{P_s \tau_e d_{ri}^\eta}{\beta_r P_r N_s d_{si}^\eta} \right)^l dd_{si} d\theta, \quad (50)
 \end{aligned}$$

and

$$\begin{aligned}
 \mathcal{J}_3 &= \int_0^\infty \int_0^\pi d_{si} \frac{\exp\left(-\frac{\tau_e \sigma_{i1}^2 d_{si}^\eta}{\beta_s P_s} - \frac{\tau_e \sigma_{i2}^2 d_{ri}^\eta}{\beta_r P_r}\right)}{(1 + \kappa_1 \tau_e)^{N_s-1}} \\
 &\quad \times (1 + \kappa_2 \tau_e)^{-(N_r-1)} \left(1 + \frac{P_s d_{ri}^\eta \tau_e}{\beta_r P_r N_s d_{si}^\eta}\right)^{-N_s} \\
 &\quad \times \sum_{p=1}^{N_e} \frac{1}{\Gamma(p)} \left(\frac{\tau_e \sigma_{i1}^2 d_{si}^\eta}{\beta_s P_s} \right)^{p-1} \sum_{q=0}^{N_e-p} \binom{N_s-1}{q} (\kappa_1 \tau_e)^q \\
 &\quad \times \sum_{m=1}^{N_e} \frac{1}{\Gamma(m)} \left(\frac{\tau_e \sigma_{i2}^2 d_{ri}^\eta}{\beta_r P_r} \right)^{m-1} \sum_{n=0}^{N_e-m} \binom{N_r-1}{n} (\kappa_2 \tau_e)^n \\
 &\quad \times \sum_{l=0}^{N_e-m-n} \binom{N_s}{l} \left(\frac{P_s d_{ri}^\eta \tau_e}{\beta_r P_r N_s d_{si}^\eta} \right)^l dd_{si} d\theta. \quad (51)
 \end{aligned}$$

In (48), the operation (a) can be justified by applying the probability generating functional (PGFL) for the PPP Φ , given by [41]

$$\mathbb{E}_\Phi \left[\prod_{x \in \Phi} f(x) \right] = \exp \left\{ - \int_{\mathbb{R}^2} [1 - f(x)] \lambda dx \right\}, \quad (52)$$

and by changing to polar coordinates.

In order to proceed with our analysis we first derive \mathcal{J}_1 as

$$\begin{aligned}
 \mathcal{J}_1 &= \pi (1 + \kappa_1 \tau_e)^{-(N_s-1)} \sum_{p=1}^{N_e} \frac{1}{\Gamma(p)} \sum_{q=0}^{N_e-p} \binom{N_s-1}{q} (\kappa_1 \tau_e)^q \\
 &\quad \times \int_0^\infty d_{si} \exp\left(-\frac{\tau_e \sigma_{i1}^2 d_{si}^\eta}{\beta_s P_s}\right) \left(\frac{\tau_e \sigma_{i1}^2 d_{si}^\eta}{\beta_s P_s} \right)^{p-1} dd_{si} \\
 &\stackrel{(b)}{=} \frac{\pi}{2} (1 + \kappa_1 \tau_e)^{-(N_s-1)} \sum_{p=1}^{N_e} \frac{1}{\Gamma(p)} \sum_{q=0}^{N_e-p} \binom{N_s-1}{q} (\kappa_1 \tau_e)^q \\
 &\quad \times \int_0^\infty \exp\left(-\frac{\tau_e \sigma_{i1}^2 u^{\frac{\eta}{2}}}{\beta_s P_s}\right) \left(\frac{\tau_e \sigma_{i1}^2 u^{\frac{\eta}{2}}}{\beta_s P_s} \right)^{p-1} du \\
 &\stackrel{(c)}{=} \frac{\pi}{\eta} \left(\frac{\beta_s P_s}{\tau_e \sigma_{i1}^2} \right)^{\frac{2}{\eta}} (1 + \kappa_1 \tau_e)^{-(N_s-1)} \\
 &\quad \times \sum_{p=1}^{N_e} \frac{1}{\Gamma(p)} \sum_{q=0}^{N_e-p} \binom{N_s-1}{q} (\kappa_1 \tau_e)^q \\
 &\quad \times \int_0^\infty \exp(-t) t^{\frac{2}{\eta}+p-1} dt \\
 &\stackrel{(d)}{=} \frac{\pi}{\eta} \left(\frac{\beta_s P_s}{\tau_e \sigma_{i1}^2} \right)^{\frac{2}{\eta}} (1 + \kappa_1 \tau_e)^{-(N_s-1)} \\
 &\quad \times \sum_{p=1}^{N_e} \frac{\Gamma\left(\frac{2}{\eta} + p - 1\right)}{\Gamma(p)} \sum_{q=0}^{N_e-p} \binom{N_s-1}{q} (\kappa_1 \tau_e)^q, \quad (53)
 \end{aligned}$$

where in (b) we use $u = d_{si}^2$, in (c) we use $t = \frac{\tau_e \sigma_{i1}^2}{\beta_s P_s} u^{\frac{\eta}{2}}$, and (d) follows from the definition of the gamma function.

Similarly, we derive \mathcal{J}_2 as

$$\begin{aligned} \mathcal{J}_2 &\stackrel{(e)}{=} (1 + \kappa_2 \tau_e)^{-(N_r-1)} \\ &\times \int_0^\infty \int_0^\pi d_{si} \frac{\exp\left(-\frac{\tau_e \sigma_{i2}^2}{\beta_r P_r} (d_{sr}^2 + d_{si}^2 - 2d_{sr}d_{si} \cos \theta)^{\frac{\eta}{2}}\right)}{\left(1 + \frac{P_s \tau_e (d_{sr}^2 + d_{si}^2 - 2d_{sr}d_{si} \cos \theta)^{\frac{\eta}{2}}}{\beta_r P_r N_s d_{si}^\eta}\right)^{N_s}} \\ &\times \sum_{m=1}^{N_e} \frac{1}{\Gamma(m)} \left(\frac{\tau_e \sigma_{i2}^2}{\beta_r P_r} (d_{sr}^2 + d_{si}^2 - 2d_{sr}d_{si} \cos \theta)^{\frac{\eta}{2}}\right)^{m-1} \\ &\times \sum_{n=0}^{N_e-m} \binom{N_r-1}{n} (\kappa_2 \tau_e)^n \sum_{l=0}^{N_e-m-n} \binom{N_s}{l} \left(\frac{P_s \tau_e}{\beta_r P_r N_s d_{si}^\eta}\right)^l \\ &\times \left((d_{sr}^2 + d_{si}^2 - 2d_{sr}d_{si} \cos \theta)^{\frac{\eta}{2}}\right)^l dd_{si} d\theta, \end{aligned} \quad (54)$$

where in (e) we apply the cosine formula. We further derive \mathcal{J}_3 as

$$\begin{aligned} \mathcal{J}_3 &= (1 + \kappa_1 \tau_e)^{-(N_s-1)} (1 + \kappa_2 \tau_e)^{-(N_r-1)} \\ &\times \int_0^\infty \int_0^\pi d_{si} \exp\left(-\frac{\tau_e \sigma_{i1}^2}{\beta_s P_s} d_{si}^\eta\right) \\ &\times \sum_{p=1}^{N_e} \frac{1}{\Gamma(p)} \left(\frac{\tau_e \sigma_{i1}^2}{\beta_s P_s} d_{si}^\eta\right)^{p-1} \sum_{q=0}^{N_e-p} \binom{N_s-1}{q} (\kappa_1 \tau_e)^q \\ &\times \frac{\exp\left(-\frac{\tau_e \sigma_{i2}^2}{\beta_r P_r} (d_{sr}^2 + d_{si}^2 - 2d_{sr}d_{si} \cos \theta)^{\frac{\eta}{2}}\right)}{\left(1 + \frac{P_s \tau_e (d_{sr}^2 + d_{si}^2 - 2d_{sr}d_{si} \cos \theta)^{\frac{\eta}{2}}}{\beta_r P_r N_s d_{si}^\eta}\right)^{N_s}} \\ &\times \sum_{m=1}^{N_e} \frac{1}{\Gamma(m)} \left(\frac{\tau_e \sigma_{i2}^2}{\beta_r P_r} (d_{sr}^2 + d_{si}^2 - 2d_{sr}d_{si} \cos \theta)^{\frac{\eta}{2}}\right)^{m-1} \\ &\times \sum_{n=0}^{N_e-m} \binom{N_r-1}{n} (\kappa_2 \tau_e)^n \sum_{l=0}^{N_e-m-n} \binom{N_s}{l} \left(\frac{P_s \tau_e}{\beta_r P_r N_s d_{si}^\eta}\right)^l \\ &\times \left((d_{sr}^2 + d_{si}^2 - 2d_{sr}d_{si} \cos \theta)^{\frac{\eta}{2}}\right)^l dd_{si} d\theta, \end{aligned} \quad (55)$$

Substituting (53), (54), and (55) into (48), we obtain the desired result in (30), which completes the proof.

REFERENCES

- [1] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29–40, Sep. 2013.
- [2] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.
- [3] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [4] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- [5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 6, pp. 3088–3104, Jul. 2010.
- [6] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.
- [7] C. Liu, G. Geraci, N. Yang, J. Yuan, and R. Malaney, "Beamforming for MIMO Gaussian channels with imperfect channel state information," in *Proc. IEEE GlobeCOM 2013*, Atlanta, USA, Dec. 2013.
- [8] C. Liu, N. Yang, G. Geraci, J. Yuan, and R. Malaney, "Secrecy in MIMOME wiretap channels: Beamforming with imperfect CSI," in *Proc. IEEE ICC 2014*, Sydney, Australia, Jun. 2014.
- [9] N. Yang, G. Geraci, J. Yuan, and R. Malaney, "Confidential broadcasting via linear precoding in non-homogeneous MIMO multiuser networks," *IEEE Trans. Commun.*, vol. 62, no. 7, pp. 2515–2530, Jul. 2014.
- [10] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.
- [11] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2170–2181, Jun. 2013.
- [12] N. Yang, S. Yan, J. Yuan, R. Malaney, R. Subramanian, and I. Land, "Artificial noise: Transmission optimization in multi-input single-output wiretap channels," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1771–1783, May 2015.
- [13] N. Yang, M. Elkashlan, T. Q. Duong, J. Yuan, and R. Malaney, "Optimal transmission with artificial noise in MISOME wiretap channels," *IEEE Trans. Veh. Technol.*, accepted to appear.
- [14] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.
- [15] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, "Physical layer security of TAS/MRC with antenna correlation," *IEEE Trans. Inf. Foren. Sec.*, vol. 8, no. 1, pp. 254–259, Jan. 2013.
- [16] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and J. Yuan, "MIMO wiretap channels: A secure transmission using transmit antenna selection and receive generalized selection combining," *IEEE Commun. Lett.*, vol. 17, no. 9, pp. 1754–1757, Sep. 2013.
- [17] S. Yan, N. Yang, R. Malaney, and J. Yuan, "Transmit antenna selection with Alamouti coding and power allocation in MIMO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1656–1667, Mar. 2014.
- [18] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.
- [19] H. Wang, X. Zhou, and M. C. Reed, "Physical layer security in cellular networks: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2776–2787, Jun. 2013.
- [20] G. Geraci, S. Singh, J. G. Andrews, J. Yuan, and I. B. Collings, "Secrecy rates in broadcast channels with confidential messages and external eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 13, no. 5, pp. 2931–2943, May 2014.
- [21] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "Physical layer security in downlink multi-antenna cellular networks," *IEEE Trans. Commun.*, vol. 62, no. 6, pp. 2006–2021, Jun. 2014.
- [22] T.-X. Zheng, H.-M. Wang, J. Yuan, D. Towsley, and M. H. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. Commun.*, accepted to appear.
- [23] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, pp. 3062–3080, Dec. 2004.
- [24] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. R. Bloch, S. Ulukus, and A. Yener, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 16–28, Sep. 2013.
- [25] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.
- [26] J. Huang, and A. Lee Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.
- [27] X. Chen, C. Zhong, C. Yuen, and H.-H. Chen, "Multi-antenna relay aided wireless physical layer security," *IEEE Commun. Mag.*, accepted to appear.
- [28] X. Chen, L. Lei, H. Zhang, and C. Yuen, "Large-scale MIMO relaying techniques for physical layer security: AF or DF?" *IEEE Trans. Wireless Commun.*, accepted to appear.
- [29] J. Chen, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inf. Foren. Sec.*, vol. 7, no. 1, pp. 310–320, Feb. 2012.

- [30] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.
- [31] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.
- [32] C. Liu, N. Yang, J. Yuan, and R. Malaney, "Location-based secure transmission for wiretap channels," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 7, pp. 1458–1470, Jul. 2015.
- [33] C. Liu, N. Yang, J. Yuan, and R. Malaney, "Secure transmission for relay wiretap channels in the presence of spatially random eavesdroppers," in *Proc. IEEE Globecom workshop on TCPLS*, San Diego, USA, Dec. 2015.
- [34] S. Weber, J. G. Andrews, and N. Jindal, "An overview of the transmission capacity of wireless networks," *IEEE Trans. Commun.*, vol. 58, no. 12, pp. 3593–3604, Dec. 2010.
- [35] P. A. Dighe, R. K. Mallik, and S. S. Jamuar, "Analysis of transmit-receive diversity in Rayleigh fading," *IEEE Trans. Commun.*, vol. 51, no. 4, pp. 674–703, Apr. 2003.
- [36] M. Kang and M.-S. Alouini, "A comparative study on the performance of MIMO MRC with and without cochannel interference," *IEEE Trans. Commun.*, vol. 52, no. 8, pp. 1417–1425, Aug. 2004.
- [37] M. R. McKay, A. J. Grant, and I. B. Collings, "Performance analysis of MIMO-MRC in double-correlated Rayleigh Environments," *IEEE Trans. Commun.*, vol. 55, no. 3, pp. 497–507, Mar. 2007.
- [38] P. A. Dighe, R. K. Mallik, and S. S. Jamuar, "Analysis of transmit-receive diversity in Rayleigh fading," *IEEE Trans. Commun.*, vol. 51, no. 4, pp. 694–703, Apr. 2003.
- [39] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th edition. Academic Press, 2007.
- [40] H. Gao, P. J. Smith, and M. V. Clark, "Theoretical reliability of MMSE linear diversity combining in Rayleigh-fading additive interference channels," *IEEE Trans. Commun.*, vol. 46, no. 5, pp. 666–672, May 1998.
- [41] D. Stoyan, W. Kendall, and J. Mecke, *Stochastic Geometry and its Applications*, 2nd ed. John Wiley & Sons Ltd., 1996.